(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 825 739 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
25.02.1998 Bulletin 1998/09

(51) Int. Cl.[6]: **H04L 9/00**, G07F 7/10

(21) Application number: **96202293.5**

(22) Date of filing: **15.08.1996**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

(71) Applicant:
Koninklijke PTT Nederland NV
2595 AL Den Haag (NL)

(72) Inventors:
- **Rombaut, Willem**
  2552 HT The Hague (NL)
- **Muller, Frank**
  2623 NJ Delft (NL)
- **Quak, Jacobus Theodorus Willem**
  3531 KD Utrecht (NL)

(74) Representative:
Beitsma, Gerhard Romano
Koninklijke PTT Nederland N.V.,
P.O. Box 95321
2509 CH Den Haag (NL)

(54) Method of loading commands in the security module of a terminal

(57) The invention provides a method of loading commands (C1, C2, ..) in a security module (2) of a terminal (1), the method comprising the steps of: a station (4) transferring the commands (C1-Cn) to the terminal (1), the terminal (1) transferring the commands (C1-Cn) to the security module (2), the security module (2) executing the commands (C1-Cn), the terminal (1) recording actual results (R1'-Rm') of the executed commands (C1-Cn), and the transfer means (3) transferring the results (R1'-Rm') back to the station (4). The commands may have associated expected results (e.g. R1), which the terminal (1) may compare with the actual results (e.g. R1'). This allows both a flexible loading of data in the security module (2) by means of commands and a remote check of the functioning of the security module.

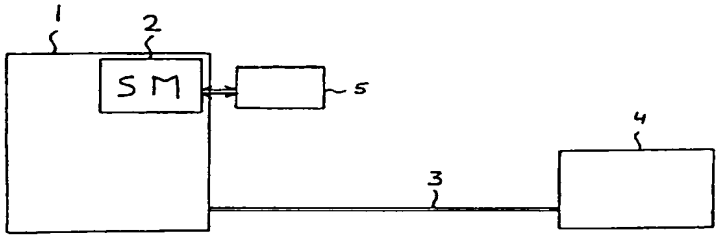

Fig. 1

EP 0 825 739 A1

Description

BACKGROUND OF THE INVENTION

The present invention relates to a method of loading commands in the security module of a terminal. More specifically, the present invention relates to the controlled loading of data in the security module of a smart card operated terminal by means of the execution of commands.

Terminals, such as vending machines or public telephones, often comprise a security module for securely storing usage data. Such payment data are e.g. the number of times the terminal has been used, the amount of money spent by consumers at the particular terminal, or the number of telephone metering pulses the (telephone) terminal has collected. A security module, which is mechanically protected against abuse, comprises electronic memory means (such as counters and EEPROM) for registering payment data and for storing keys. A security module may further comprise processing means for processing data, such as usage data. Such processing means normally comprise a microprocessor running programs consisting of commands stored in the security module. The processing often comprises the cryptographic protection of the usage data in order to prevent fraud.

It is often necessary to update the data stored in a security module, e.g. for adding new functions or modifying existing functions. Data may be added or altered using commands, the execution of which effects the desired addition or alteration. However, the functioning of the additions and alterations needs to be verified. This is especially true since security modules often store monetary data or their equivalents.

Thus the need arises to be able to load such new data into the security module and to verify their effects, i.e. the proper functioning of the modifications brought about by those data. As in practice it will be necessary to effect changes in security modules in many different locations, verifying the functioning of those security modules constitutes a problem. The Prior Art does not offer a solution for this problem.

SUMMARY OF THE INVENTION

It is an object of the invention to overcome the above-mentioned and other disadvantages of the prior art and to provide a method which allows data to be loaded into the security module of a terminal and to verify the proper functioning of the commands using those data. It is a further object of the invention to provide a method which allows the remote function check of a security module. It is another object of the present invention to provide a method which allows the terminal to be transparant with respect to the commands.

Accordingly, the present invention provides a method of loading commands in a security module of a terminal, the method comprising the steps of:

- a station transferring the commands to the terminal via a transfer means,
- the terminal transferring the commands to the security module,
- the security module executing the commands,
- the terminal recording results of the executed commands, and
- the transfer means transferring the results to the station.

The station may be a remote terminal management agency. The transfer means may e.g. be a telephone line or a (special purpose) card which is inserted into the terminal.

By recording the results of the executed commands, it is possible to remotely check the proper functioning of the security module. Preferably, the commands are transferred to the terminal as part of a script file, the terminal extracting the respective commands from the script file and passing them to the security module. Advantageously the script file contains information allowing the selective recording of results, i.e. allowing the results of some commands to be registered, while the result of other commands are not registered. This makes it possible to control the loading of certain commands into the security module by requiring the proper execution of the previous command, while allowing other commands (e.g. commands of which the results are unpredictable) to be loaded without imposing a restriction.

As the terminal substantially only transfers the commands to the secure module, the terminal is effectively transparant with respect to the commands. This makes the terminal substantially independent of the particular security module used.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will further be explained with reference to the accompanying drawings, in which:

Fig. 1 schematically shows a terminal in which the method of the present invention may be used,
Fig. 2 schematically shows an example of the structure of a script file containing commands to be loaded.

EXEMPLARY EMBODIMENTS

The embodiment shown schematically and by way of example in Fig. 1 comprises a terminal 1, connected via a telephone link 3 with a station (terminal management centre) 4. As will be explained below, the station 4 may serve both to make script files and to verify the functioning of the terminal 1. The terminal 1 comprises at least one security module 2 which during normal use

of the terminal 1 communicates with a smart card 5.

In order to load commands and execute into the security module 2 while having the possibility to check their proper functioning, as provided by the present invention, a script file is made in the station 4. The script file, which will further be explained with reference to Fig. 2, contains the commands to be loaded and executed, thus effecting a data transfer to and/or from the security module 2. Preferably, the terminal 1 verifies the origin of the commands, i.e. the terminal checks whether the commands were produced by or at least sent by the station 4. This verification, which serves to prevent fraudulent modifications of the contents of the security module, may be effected by comparing a received MAC (message authentication code) with a MAC calculated by the terminal. Such verfication procedures are well known in the art.

As shown in Fig. 2, a script file S may contain a header H and a number of records, each record comprising a type field Ti (e.g. T1), a command field Ci (e.g. C1) and a result field Ri (e.g. R1). The result field Ri may be empty, as will be explained later. A command may contain data to be written in the memory of the security module, such as a key for encrypting usage data. However, a command may also contain an instruction to be executed by the security module 2. A suitable format of the commands Ci (i ranges from 1 to 4 in Fig. 2) is e.g. disclosed in the ISO7816-4 standard.

The type field Ti allows different types of commands to be distinguished. In the method of the present invention, three different types of commands can be distinguished, resulting in three different types of command handling by the terminal.

A first type of command has an associated expected result or response R. This type of command is preferably loaded one by one in the security module, the terminal comparing the actual result Ri' with the expected result Ri and stopping the loading if a discrepancy, i.e. a mismatch between Ri and Ri' occurs. With this type of command it is possible to perform a controlled loading of the security module and to check the proper functioning of the security module while loading.

A second type of command is not accompanied by an expected response (i.e. the response field Ri may be empty). However, the terminal preferably registers the actual responses. This type of command allows a test of the security module to be performed, especially in the case where an unknown type of security module (of which the responses are not completely known in advance) is used. The results may be entered in a log file which card be collected later. Thus an off-line processing of the commands is possible.

A third type of command is loaded into the security module without taking the result into account. That is, the result of this type of command is not registered by the terminal.

It will be understood that the above-mentioned results of the commands may comprise memory contents, a status (e.g. indicating a failed write operation), and/or a smart card command. The said commands may thus effect a data transfer to and/or from the security module.

As explained above, the terminal extracts the commands from the script file and passes them to the security module. Although the terminal is passive with respect to the commands, it is active with respect to the script file in that it extracts the commands from the file and derives its mode of operation (check result/no check) from the type fields contained in the script file. The script file thus comprises information which influences the functioning of the terminal with respect to the script file and the commands derived from it.

The script file may comprise only a single command. However, the size of the script file may vary and is limited only by the amount of memory available in the terminal. It can also be envisaged that the script file contains commands in a compressed and/or cryptographically protected form.

The method of the present invention thus allows both a flexible loading of data in the security module and a remote check of the functioning of the security module.

It will be understood by those skilled in the art that the embodiments described above are given by way of example only and that many modifications and additions are possible without departing from the scope of the present invention.

Claims

1. Method of loading commands (C1, C2, ..) in a security module (2) of a terminal (1), the method comprising the steps of:

   - a station (4) transferring the commands (C1-Cn) to the terminal (1) via a transfer means (3),
   - the terminal (1) transferring the commands (C1-Cn) to the security module (2),
   - the security module (2) executing the commands (C1-Cn),
   - the terminal (1) recording results (R1'-Rm') of the executed commands (C1-Cn),and
   - the transfer means (3) transferring the results (R1'-Rm') to the station (4).

2. Method according to claim 1, wherein the commands are transferred to the terminal (1) as part of a script file (S), the terminal (1) extracting the respective commands (C1-Cn)from the script file (S) and passing them to the security module (2).

3. Method according to claim 2, wherein the script file (S) contains information (T1-Tn) allowing the selective recording of results (R1'-Rm').

4. Method according to claim 2 or 3, wherein the script

file (S) is made in the verification station (4).

5. Method according to any of the preceding claims, wherein the script file (S) contains the expected result (e.g. R3) of each command (e.g. C3).

6. Method according to claim 5, wherein each command (e.g. C1) is transferred to the security module (2) individually, the terminal (1) comparing the expected result (e.g. R3) with the actual result (e.g. R3') and stopping the transferring if a mismatch is detected.

7. Method according to any of the preceding claims, wherein the transfer means (3) is a telecommunications link, such as a telephone connection.

8. Method according to any of the preceding claims, wherein the transfer means (3) comprises a card to be inserted in the terminal (1).

9. Method according to any of the preceding claims, wherein the terminal (1), before transferring the commands (C1-Cn)to the security module (2), verifies whether the commands originate from the station (4).

10. Terminal (1) comprising a security module (2), characterized in that the terminal (1) comprises means for registering results (R1-Rm) of commands (C1-Cn)executed by the security module (2).

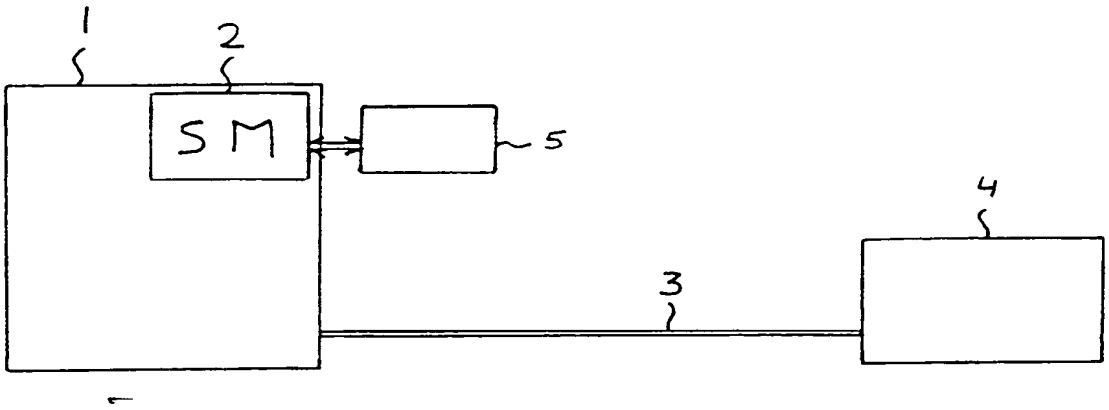

Fig. 1

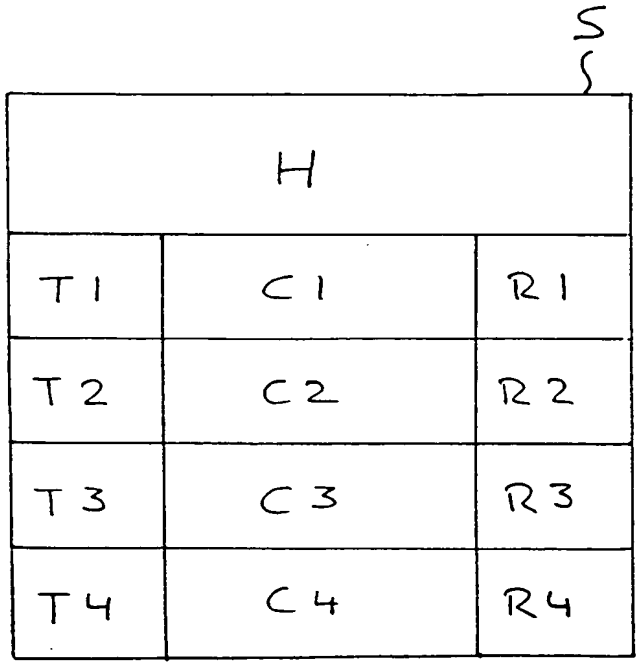

Fig. 2

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 96 20 2293

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X Y	US-A-4 972 478 (DABBISH) * column 1, line 35 - column 2, line 7 * * column 3, line 37 - line 46 * ---	1,10 2	H04L9/00 G07F7/10
Y	US-A-5 495 571 (CORRIE ET AL.) * column 2, line 29 - line 44 * * column 3, line 44 - line 57 * * column 4, line 19 - line 26 * * column 6, line 36 - line 47 * ---	2	
A	FR-A-2 657 445 (GEMPLUS) * page 2, line 30 - page 3, line 15 * * page 4, line 16 - page 5, line 22 * ---	1,7,8	-
A	EP-A-0 368 752 (BULL CP8) * column 2, line 41 - column 3, line 26 * * column 4, line 56 - column 5, line 6 * * column 6, line 18 - line 58 * ---	1,9	
A	US-A-4 777 355 (TAKAHIRA) * column 2, line 7 - line 27 * * column 3, line 24 - line 38 * * column 5, line 36 - column 6, line 11 * -----	1,6,10	

TECHNICAL FIELDS SEARCHED (Int.Cl.6)
H04L G07F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	9 January 1997	Holper, G

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)